CLAIMS:

1. An apparatus **107** for monitoring and auditing activity of a legacy environment, the apparatus comprising:

an analyzer **303** operative to analyze intercepted packets conveyed by entities **102, 103, 104** in a network and to generate analyzed data based on information associated with at least some of said packets, the analyzed data being indicative of sessions; and

a mirror manager **305** responsive to said analyzed data for generating data representative of mirror sessions, each mirror session corresponding to a session.

2. The apparatus of Claim 1, wherein the analyzer is operative to analyze headers and contents of said intercepted packets.

3. The apparatus of Claims 1 or 2, further comprising:

an audit event analyzer **307** for processing at least part of said data representative of mirror sessions and generating data representative of audit events.

4. The apparatus of Claim 3, wherein each one of said audit events is respective of operations performed by a user of said legacy environment.

5. The apparatus of Claim 3, further comprising:

a business event analyzer for processing at least part of said data representative of audit events and generating data representative of business events.

6. The apparatus of Claim 5, further comprising:

an alerts manager **312** coupled to the business event analyzer and being responsive to said data representative of business events for generating alerts.

7. The apparatus of Claim 6, wherein the alerts manager generates at least some of the alerts based on predetermined thresholds.

8. The apparatus of any one of the preceding claims, wherein said entities include hosts **103** and terminals **102**.

9. The apparatus of any one of the preceding claims further comprising:

a first long term storage device **304** for storing at least part of said analyzed data.

10. The apparatus of any one of the preceding claims further comprising:

a second long term storage device **306** for storing at least part of said data representative of mirror sessions.

11. The apparatus of any one of Claims 1 to 9, further comprising:

a compression agent **313** for compressing at least part of the data representative of mirror sessions.

12. The apparatus of claim 10, further comprising:

a compression agent **313** for compressing at least part of the data representative of mirror sessions.

13. The apparatus of Claim 12, wherein the compression agent **313** is configured to compress the data representative of mirror sessions before storing at least part of them in the second long term storage device.

14. The apparatus of any one of Claims 1 to 9 or 11, further comprising:

an encryption agent **314** for encrypting at least part of the data representative of mirror sessions.

15. The apparatus of any one of Claims 10 , 12 or 13, further comprising:

an encryption agent **314** for encrypting at least part of the data representative of mirror sessions.

16. The apparatus of Claim 15, wherein the encryption agent **314** encrypts the data representative of mirror sessions before storing at least part of them in the second long term storage device.

17. The apparatus of any one of Claims 1 to 9, 11 or 14, further comprising:

a signature agent **315** for digitally signing at least part of the data representative of mirror sessions.

18. The apparatus of any one of Claims 10 , 12, 13, 15 or 16, further comprising:

a signature agent **315** for digitally signing at least part of the data representative of mirror sessions.

19. The apparatus of Claim 18, wherein the signature agent **315** signs the data representative of mirror sessions before storing at least part of them in the second long term storage device.

20. A method for monitoring and auditing activity of a legacy environment, the method comprising:

analyzing **202** intercepted packets conveyed by entities in a network;

generating **203** analyzed data based on information associated with at least some of said packets, the analyzed data being indicative of sessions; and

responsive to said analyzed data generating **204** in respect of each one of one or more of said sessions data representative of a mirror session, each mirror session corresponds to a session.

21. The method of Claim 20, wherein analyzing intercepted packets includes analyzing headers and contents of said packets.

22. The method of Claims 20 or 21, further comprising:

processing at least part of said data representative of mirror sessions and generating **206** data representative of audit events.

23. The method of Claim 22, wherein each one of said audit events is respective of operations performed by a user of said legacy environment.

24. The method of Claim 22, further comprising:

processing at least part of said data representative of audit events and generating **207** data representative of business events.

25. The method of Claim 24, further comprising:

responsive to said data representative of business events generating alerts in respect of at least one of said business events.

26. The method of Claim 25, wherein generating at least some of the alerts is based on predetermined thresholds.

27. The method of any one of Claims 20 to 26, further comprising:

storing **205** at least part of the analyzed data in a first long term storage device.

28. The method of any one of Claims 20 to 27, further comprising:

storing **208** at least part of the data representative of mirror sessions in a second long term storage device.

29. The method of Claims 20 to 27, further comprising:

compressing **211** at least part of said data representative of mirror sessions.

30. The method of Claim 28, further comprising:

compressing **211** at least part of said data representative of mirror sessions.

31. The method of Claim 30, wherein the compressing **211** the at least part of said data representative of mirror sessions is performed before storing **208** at least part of them in the second long term storage device.

32. The method of any one of Claims 20 to 27 or 29, further comprising:

encrypting **212** at least part of said data representative of mirror sessions.

33. The method of any one of Claims 28, 30 or 31 further comprising:

encrypting **212** at least part of said data representative of mirror sessions.

34. The method of Claim 33, wherein the encrypting **212** the at least part of said data representative of mirror sessions is performed before storing **208** at least part of them in the second long term storage device.

35. The method of any one of Claims 20 to 27, 29 or 32, further comprising:

digitally signing **213** at least part of said data representative of mirror sessions.

36. The method of any one of Claims 28, 30, 31, 33 or 34, further comprising:

digitally signing **213** at least part of said data representative of mirror sessions.

37. The method of Claim 36, wherein the digitally signing **213** the at least part of said data representative of mirror sessions is performed before storing **208** at least part of them in the second long term storage device.